

Hi Hackers!! Today we will be doing swagshop. Another linux based box with tons to explore. Lets begin this journey!!

Enumeration

Starting with the nmap scan:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b6:55:2b:d2:4e:8f:a3:81:72:61:37:9a:12:f6:24:ec (RSA)
|   256  2e:30:00:7a:92:f0:89:30:59:c1:77:56:ad:51:c0:ba (ECDSA)
|_  256  4c:50:d5:f2:70:c5:fd:c4:b2:f0:bc:42:20:32:64:34 (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Home page
|_ http-favicon: Unknown favicon MD5: 88733EE53676A47FC354A61C32516E82
| http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Just two ports running, now we don't have to think about this box much. We will start with port 80 because from there we will get our shell.

Port 80

The home page is something like this:

HOME PAGE

[COMPARE PRODUCTS](#)

You have no items to compare.

NEW PRODUCTS

1.  5 X HACK THE BOX STICKER
2.  5 X HACK THE BOX SQUARE STICKER
3.  HACK THE BOX LOGO T-SHIRT

COMPANY

[ABOUT US](#)
[CONTACT US](#)
[CUSTOMER SERVICE](#)
[PRIVACY POLICY](#)

QUICK LINKS

[SITE MAP](#)
[SEARCH TERMS](#)
[ADVANCED SEARCH](#)

ACCOUNT

[MY ACCOUNT](#)
[ORDERS AND RETURNS](#)

NEWSLETTER

[SUBSCRIBE](#)

Going through the website, we can register and create a new account, also we can look at our account settings. Additionally we can add items in the cart and checkout. That's the basic functionality of this ecommerce site. Looking at the wappalyzer extension output, we can see programming languages being used is PHP, Database running is MySQL and the webserver is Apache.

The ecommerce site running is quite old, you will notice that below:

© 2014 Magento Demo Store. All Rights Reserved.

Running a quick searchsploit on magento, there are two relevant exploits we could have a look at.

```
(root@kali)-[/home/rishabh/HTB/swagshop]
```

```
# searchsploit magento
```

```
1 0
```

```
-----
```

```
Exploit Title
```

```
| Path
```

```
-----
```

```
-----
```

```
eBay Magento 1.9.2.1 - PHP FPM XML eXternal Entity Injection
```

```
| php/webapps/38573.txt
```

```
eBay Magento CE 1.9.2.1 - Unrestricted Cron Script (Code Execution / Denial of
```

```

Ser | php/webapps/38651.txt
Magento 1.2 - '/app/code/core/Mage/Admin/Model/Session.php?login['Username']'
Cros | php/webapps/32808.txt
Magento 1.2 - '/app/code/core/Mage/Adminhtml/controllers/IndexController.php?email | php/webapps/32809.txt
Magento 1.2 - 'downloader/index.php' Cross-Site Scripting
| php/webapps/32810.txt
Magento < 2.0.6 - Arbitrary Unserialize / Arbitrary Write File
| php/webapps/39838.php
Magento CE < 1.9.0.1 - (Authenticated) Remote Code Execution
| php/webapps/37811.py
Magento eCommerce - Local File Disclosure
| php/webapps/19793.txt
Magento eCommerce - Remote Code Execution
| xml/webapps/37977.py
Magento Server MAGMI Plugin - Multiple Vulnerabilities
| php/webapps/35996.txt
Magento Server MAGMI Plugin 0.7.17a - Remote File Inclusion
| php/webapps/35052.txt
Magento WooCommerce CardGate Payment Gateway 2.0.30 - Payment Process Bypass
| php/webapps/48135.php
-----
----
Shellcodes: No Results

```

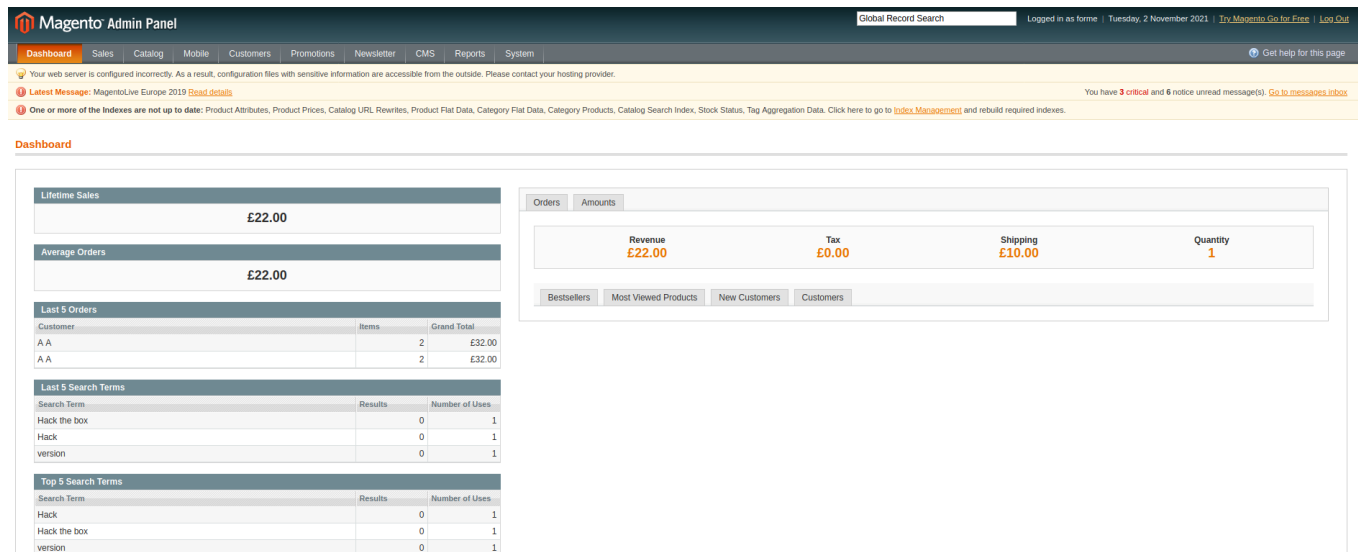
I copied the Magento E-commerce Remote Code execution and changed the target to "<http://swagshop.htb/index.php>". You will see the output something like this.

```

└─(root@kali)-[/home/rishabh/HTB/swagshop]
└─# python exploit.py
1 ✎
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-
any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no
longer supported by the Python core team. Support for it is now deprecated in
cryptography, and will be removed in the next release.
WORKED
Check http://swagshop.htb/index.php/admin with creds forme:forme

```

Now go to the link as shown and enter username "forme" and password "forme". You will be presented a page like this:



The screenshot shows the Magento Admin Panel Dashboard. The top navigation bar includes links for Dashboard, Sales, Catalog, Mobile, Customers, Promotions, Newsletter, CMS, Reports, and System. The dashboard displays several key metrics and tables:

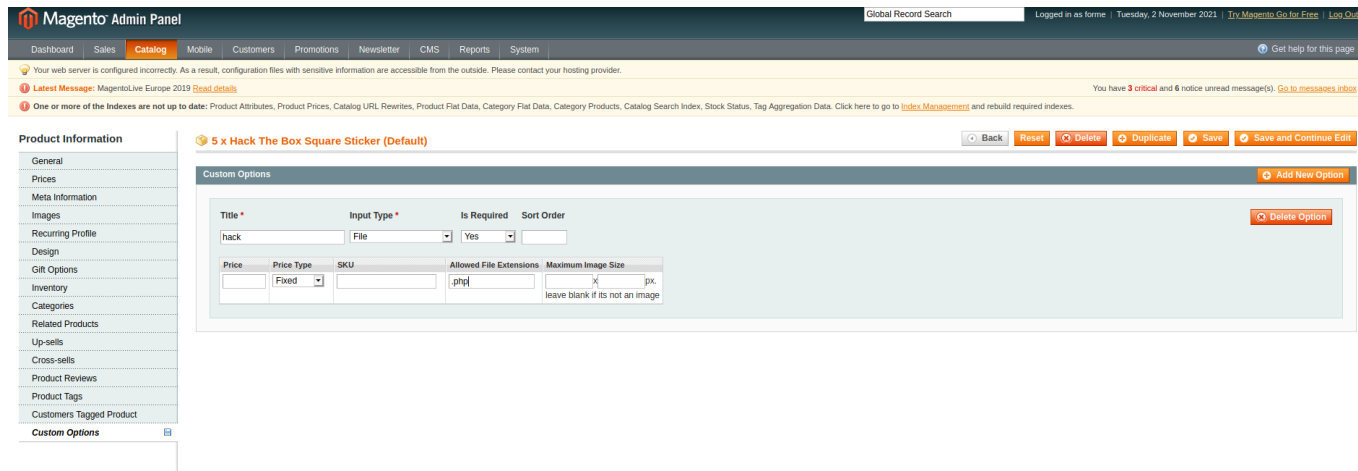
- Lifetime Sales:** £22.00
- Average Orders:** £22.00
- Last 5 Orders:** A table with columns for Customer, Items, and Grand Total. It shows two orders for customer 'A A' with 2 items each, totaling £32.00.
- Last 5 Search Terms:** A table with columns for Search Term, Results, and Number of Uses. It shows three search terms: 'Hack the box' (0 results, 1 use), 'Hack' (0 results, 1 use), and 'version' (0 results, 1 use).
- Top 5 Search Terms:** A table with columns for Search Term, Results, and Number of Uses. It shows three search terms: 'Hack' (0 results, 1 use), 'Hack the box' (0 results, 1 use), and 'version' (0 results, 1 use).

On the right side, there is a summary of orders and amounts, showing Revenue (£22.00), Tax (£0.00), Shipping (£10.00), and Quantity (1). Below this, there are tabs for Bestsellers, Most Viewed Products, New Customers, and Customers.

At the bottom, you can note down the version info which is Magento ver. 1.9.0.0. For this version, there is an authenticated remote code execution vulnerability. I modified the exploit many times, but it was throwing an error. I then moved to another method which is documented well here: <https://blog.scrt.ch/2019/01/24/magento-rce-local-file-read-with-low-privilege-admin-rights/>

Initial Foothold

In the admin panel go to catalog → select manage products → click edit on any of the products → Select custom options and Add new. You will get a window something similar to this:



The screenshot shows the Magento Admin Panel Custom Options form. The left sidebar contains a list of product information sections: General, Prices, Meta Information, Images, Recurring Profile, Design, Gift Options, Inventory, Categories, Related Products, Up-sells, Cross-sells, Product Reviews, Product Tags, Customers Tagged Product, and Custom Options. The main content area displays the 'Custom Options' form for a product titled '5 x Hack The Box Square Sticker (Default)'. The form includes fields for Title, Input Type, Is Required, Sort Order, Price, Price Type, SKU, Allowed File Extensions, and Maximum Image Size. The 'Title' field is set to 'hack', 'Input Type' is 'File', 'Is Required' is 'Yes', and 'Sort Order' is '1'. The 'Price' field is set to 'Fixed', 'SKU' is empty, 'Allowed File Extensions' is '.php', and 'Maximum Image Size' is '1024x1024px'. The form also includes buttons for Back, Reset, Delete, Duplicate, Save, and Save and Continue Edit.

Now Input type should be set to file, and allowed file extensions should be set to .php and also add price as anything. Click on save and you will get a message something similar to this: "The product has been saved"

Now go to the new products page where all the products are selected and click on the product you edited. You will see a file upload button like this:

5 X HACK THE BOX STICKER £4.00

IN STOCK

Official Hack The Box Stickers. Take home this 5x HTB sticker pack to stick on all your favorite electronics. Its the perfect size to hide the Apple logo and show the world who's the real deal.

filehacks * +£1.00

* Required Fields

Browse...

No file selected.


Allowed file extensions to upload: .php


Qty:


ADD TO CART

[Add to Wishlist](#)



[Add to Compare](#)







Upload your php shell by clicking on browse and add to cart. Once added you will see a page like this

PRODUCT	PRICE	QTY	SUBTOTAL	
	5 X HACK THE BOX STICKER SKU: HTB-003-123	£5.00	<input type="text" value="1"/> Edit	£5.00 
<div>filehacks: <input type="text" value="shell.php"/></div>				
EMPTY CART		UPDATE SHOPPING CART -OR- CONTINUE SHOPPING		

You can checkout as guest, once you see this page:

YOUR ORDER HAS BEEN RECEIVED.

THANK YOU FOR YOUR PURCHASE!

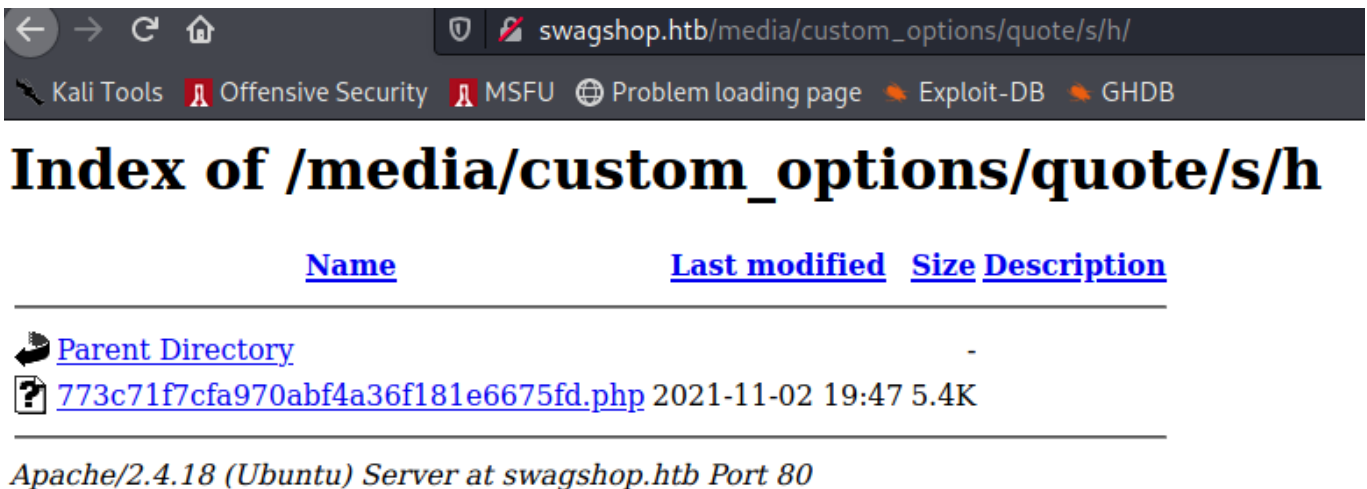
Your order # is: [100000003](#).



You will receive an order confirmation email with details of your order and a link to track its progress.

Click [here to print](#) a copy of your order confirmation.

CONTINUE SHOPPING

According to the article, your file has been uploaded successfully, now go to `/media/custom_options/quote/firstLetterofYourFilename/secondLetterofYourFilename/`. As directory listing is allowed, you will see your file sitting there. In my case, I have uploaded a file called `shell.php`. So I navigate to `/media/custom_options/quote/s/h/`



<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 773c71f7cfa970abf4a36f181e6675fd.php	2021-11-02 19:47	5.4K	

Apache/2.4.18 (Ubuntu) Server at swagshop.htb Port 80

Set up the listener and you will get the shell back as `www-data` user.

```
(root@kali) - [ /home/rishabh/HTB/swagshop ]
# r1wrap nc -nvlp 8989
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::8989
Ncat: Listening on 0.0.0.0:8989
Ncat: Connection from 10.129.95.151.
Ncat: Connection from 10.129.95.151:49148.
Linux swagshop 4.4.0-146-generic #172-Ubuntu SMP Wed Apr 3 09:00:08 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
19:55:42 up 2:49, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
uid
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Privilege Escalation

User www-data can run sudo using vi on any of the files `"/var/www/html/*"`

```

sudo -l
Matching Defaults entries for www-data on swagshop:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on swagshop:
    (root) NOPASSWD: /usr/bin/vi /var/www/html/*

```

Change to tty shell. Create any file using touch command in /var/www/html directory because that is where www-data user has write permissions. Now run this command:

```
sudo /usr/bin/vi /var/www/html/file
```

[illegible]

Voila!! You have root shell. Thats it guys. It was definitely not a easy box. Research was required but it was a good learning experience. See you tomorrow.